IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	§	Group Art Unit: 2163
Susann M. Keohane, *et al.*	§	
	§	Examiner: Phan, Tuankhanh D.
Serial No.: 10/677,660	§	
	§	Atty Docket No.: AUS920030640US1
Filed: 10/02/2003	§	
	§	Customer No.: 60501
Title: Providing A Necessary Level Of	§	
Security For Computers Capable Of	§	Confirmation No.: 9966
Connecting To Different Computing	§	
Environments	§	

Mail Stop: Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPEAL BRIEF

Honorable Commissioner:

This is an Appeal Brief filed pursuant to 37 CFR § 41.37 in response to the Final Office Action of July 17, 2008 (hereafter "the Office Action") and pursuant to the Notice of Appeal filed October 16, 2008.

REAL PARTY IN INTEREST

The real party in interest in accordance with 37 CFR § 41.37(c)(1)(i) is the patent assignee, Lenovo (Singapore) PTE Ltd. ("Lenovo").

RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences within the meaning of 37 CFR § 41.37(c)(1)(ii).

STATUS OF CLAIMS

Status of claims in accordance with 37 CFR § 41.37(c)(1)(iii): Thirty nine claims are filed in the original application in this case. Claim 1-39 are on appeal.

STATUS OF AMENDMENTS

Status of amendments in accordance with 37 CFR § 41.37(c)(1)(iv): No amendments were submitted after final rejection. The claims as currently presented are included in the Appendix of Claims that accompanies this Appeal Brief.

SUMMARY OF CLAIMED SUBJECT MATTER

Appellants provide the following summary of the claimed subject matter according to 37 CFR § 41.37(c)(1)(v). This summary includes a concise explanation of the subject matter defined in each of the independent claims involved in the appeal and includes references to Appellants' original specification by page and line number and to the drawings by reference characters. The independent claims involved in this appeal are claims 1, 11, 14, 24, 27, and 37. Claims 1, 14, and 27 recite corresponding method, system, and computer program product aspects of providing a necessary level of security for a computer capable of connecting to different computing environments. Claims 11, 24, and 37 recite other corresponding method, system, and computer program product aspects of providing a necessary level of security for a computer capable of connecting to different computing environments.

Claim 1 recites a method for providing a necessary level of security for a computer capable of connecting to different computing environments including monitoring a type of connection between the computer and a network in a current computing environment (page 15, lines 3-13, and Figure 5, element 402). The method of claim 1 also includes determining a security level of data before sending the data across the network (page 16, lines 19-25 and Figure 5, elements 406 and 408). The method of claim 1 also includes storing the data in a buffer instead of sending the data across the network if the connection to the network lacks a security control required for the determined security level of the data (page 20, lines 4-6 and Figure 5, elements 410 and 416). The method of claim 1 also includes sending the data from the buffer when the computer is connected to a changed computing environment having a new type of connection that has the security control required for the data (page 20, lines 6-9, and Figure 5, elements 420 and 412).

Claim 14 recites a system for providing a necessary level of security for a computer capable of connecting to different computing environments including means for monitoring a type of connection between the computer and a network in a current computing environment (page 15, lines 3-13, and Figure 5, element 402). The system of claim 14 also includes means for determining a security level of data before sending the data across the network (page 16, lines 19-25 and Figure 5, elements 406 and 408). The system of claim 14 also includes means for storing the data in a buffer instead of sending the data across the network if the connection to the network lacks a security control required for the determined security level of the data (page 20, lines 4-6 and Figure 5, elements 410 and 416). The system of claim 14 also includes means for sending the data from the buffer when the computer is connected to a changed computing environment having a new type of connection that has the security control required for the data (page 20, lines 6-9, and Figure 5, elements 420 and 412).

Claim 27 recites a computer program product for providing a necessary level of security for a computer capable of connecting to different computing environments including a recording medium (page 6, line 18 – page 7, line 2). The computer program product of claim 27 also includes means recorded on the recording medium for monitoring a type of connection between the computer and a network in a current computing environment (page 15, lines 3-13, and Figure 5, element 402). The computer program product of claim 27 also includes means recorded on the recording medium for determining a security level of data before sending the data across the network (page 16, lines 19-25 and Figure 5, elements 406 and 408). The computer program product of claim 27 also includes means recorded on the recording medium for storing the data in a buffer instead of sending the data across the network if the connection to the network lacks a security control required for the determined security level of the data (page 20, lines 4-6 and Figure 5, elements 410 and 416). The computer program product of claim 27 also includes means recorded on the recording medium for sending the data from the buffer when the computer is connected to a changed computing environment having a new type of connection that has the security control required for the data (page 20, lines 6-9, and Figure 5, elements 420 and 412).

Claim 11 recites a method for providing a necessary level of security for a computer capable of connecting to different computing environments including connecting the computer to a network in a first computing environment (page 20, lines 6-25, Figure 5, elements 420 and 412, and Figure 1, elements 126, 134, and 132). The method of claim 11 also includes specifying a security level for data to be sent across the network (page 14, lines 4-18, and Figure 4, elements 322, 324. 326, 328, 330, and 332). The method of claim 11 also includes instructing a sending program to send the data across the network (page 13, line 14 – page 14, line 26, and Figure 4, elements 302, 304, 308, 310, 334, et al.). The method of claim 11 also includes receiving an indication that security control of the first computing environment lacks a security control required for the specified security level (page 24, line 21 – page 25, line 4, and Figures 1 and 4, elements 160, 130, 132, and 302). The method of claim 11 also includes connecting the computer to the network in a second computing environment, wherein the second computing environment has the security control required for the specified security level (page 25, lines 6-16, and Figures 1 and 4, elements 162, 130, 102, 134, and 136). The method of claim 11 also includes receiving an indication that the data has been sent across the network (page 25, line 12-16, and Figures 1 and 4, elements 162, 130, 102, 134, and 136).

Claim 24 recites a system for providing a necessary level of security for a computer capable of connecting to different computing environments including means for connecting the computer to a network in a first computing environment (page 20, lines 6-25, Figure 5, elements 420 and 412, and Figure 1, elements 126, 134, and 132). The system of claim 24 also includes means for specifying a security level for data to be sent across the network (page 14, lines 4-18, and Figure 4, elements 322, 324. 326, 328, 330, and 332). The system of claim 24 also includes means for instructing a sending program to send the data across the network (page 13, line 14 – page 14, line 26, and Figure 4, elements 302, 304, 308, 310, 334, et al.). The system of claim 24 also includes means for receiving an indication that security control of the first computing environment lacks a security control required for the specified security level (page 24, line 21 – page 25, line 4, and Figures 1 and 4, elements 160, 130, 132, and 302). The system of claim 24 also includes means for connecting the computer to the network in a second computing environment, wherein the second computing environment has the security control required for the specified security level (page 25, lines 6-16, and Figures 1 and 4, elements 162, 130, 102, 134, and 136). The system of claim 24 also includes means for receiving an indication that the data has been sent across the network (page 25, line 12-16, and Figures 1 and 4, elements 162, 130, 102, 134, and 136).

Claim 37 recites a computer program product for providing a necessary level of security for a computer capable of connecting to different computing environments including a recording medium (page 6, line 18 – page 7, line 2). The computer program product of claim 37 also includes means, recorded on the recording medium, for connecting the computer to a network in a first computing environment (page 20, lines 6-25, Figure 5, elements 420 and 412, and Figure 1, elements 126, 134, and 132). The computer program product of claim 37 also includes means, recorded on the recording medium, for specifying a security level for data to be sent across the network (page 14, lines 4-18, and Figure 4, elements 322, 324. 326, 328, 330, and 332). The computer program product of claim 37 also includes means, recorded on the recording medium, for instructing a sending program to send the data across the network (page 13, line 14 – page 14, line 26, and Figure 4, elements 302, 304, 308, 310, 334, et al.). The computer program product of claim 37 also includes means, recorded on the recording medium, for receiving an indication that security control of the first computing environment lacks a security control required for the specified security level (page 24, line 21 – page 25, line 4, and Figures 1 and 4, elements 160, 130, 132, and 302). The computer program product of claim 37 also includes means, recorded on the recording medium, for connecting the computer to the network in a second computing environment, wherein the second computing environment has the security control required for the specified security level (page 25, lines 6-16, and Figures 1 and 4, elements 162, 130, 102, 134, and 136). The computer program product of claim 37 also includes means, recorded on the recording medium, for receiving an indication that the data has been sent across the network (page 25, line 12-16, and Figures 1 and 4, elements 162, 130, 102, 134, and 136).

GROUNDS OF REJECTION

In accordance with 37 CFR § 41.37(c)(1)(vi), Appellants provide the following concise statement of each ground of rejection:

1. Claims 1-39 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Herrero, *et al.* (WO 2000/74345) in view of Holden, *et al.* (U.S. Patent No. 5,828,832).

2. Claims 1, 14, and 27 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Herrero, *et al.* (WO 2000/74345) in view of Ueda, *et al.* (U.S. Patent No. 5,692,179).

ARGUMENT

Appellants present the following arguments pursuant to 37 CFR § 41.37(c)(1)(vii) regarding the grounds of rejection in the present case.

Argument Regarding The First Ground Of Rejection: Claims 1-39 Are Rejected Under 35 U.S.C. § 103(A) As Being Unpatentable Over Herrero In View Of Holden

Claims 1-39 stand rejected for obviousness under 35 U.S.C § 103(a) as being unpatentable over Herrero, *et al.*, (WIPO WO 00/74345) (hereafter 'Herrero') in view of Holden, *et al.*, (U.S. Patent No. 5,828,832) (hereafter 'Holden'). The question of whether Applicants claims are obvious or not is examined in light of: (1) the scope and content of the prior art; (2) the differences between the claimed invention and the prior art; (3) the level of ordinary skill in the art; and (4) any relevant secondary considerations, including commercial success, long felt but unsolved needs, and failure of others. *KSR Int'l Co. v. Teleflex Inc.*, 127 S.Ct. 1727, 1729-1730, 82 USPQ 1385 (2007). Although Applicants recognize that such an inquiry is an expansive and flexible one, the Office Action must nevertheless demonstrate a prima facie case of obviousness to reject Applicants claims under for obviousness under 35 U.S.C. § 103(a). *In re Khan*, 441 F.3d 977, 985-86 (Fed. Cir. 2006). To establish a prima facie case of obviousness, the proposed combination of Herrero and Holden must teach or suggest all of Applicants' claim limitations. MPEP 2142 (citing *In re Royka*, 490 F.2d 981, 985, 180 USPQ 580, 583 (CCPA 1974)). As shown below in more detail, the proposed combination of Herrero and Holden cannot establish a prima facie case of obviousness because the proposed combination does not teach each and every element of the claims of the present application. As such, Applicants respectfully traverse each rejection individually.

The Proposed Combination Of Herrero And Holden Does Not Teach Or Suggest Each And Every Element Of Claim 1 Of The Present Application

Independent claim 1 of the present application recites:

> 1. A method for providing a necessary level of security for a computer capable of connecting to different computing environments, the method comprising:
>
> monitoring a type of connection between the computer and a network in a current computing environment;
>
> determining a security level of data before sending the data across the network;
>
> storing the data in a buffer instead of sending the data across the network if the connection to the network lacks a security control required for the determined security level of the data; and
>
> sending the data from the buffer when the computer is connected to a changed computing environment having a new type of connection that has the security control required for the data.

Holden Neither Discloses Nor Suggests Storing The Data In A Buffer Or Sending the Data From The Buffer

The Office Action admits that Herrero does not disclose the third and fourth elements of claim 1 of the present application and to cure this deficiency of Herrero, takes the position that Holden at column 11, lines 28-30, column 11, lines 30-31, and column 11, lines 50-52 discloses these elements:

> storing the data in a buffer instead of sending the data across the network if the connection to the network lacks a security control required for the determined security level of the data; and
>
> sending the data from the buffer when the computer is connected to a changed computing environment having a new type of connection that has the security control required for the data.

Appellants respectfully note in response, however that what Holden at the paragraph including column 11, lines 28-30, column 11, lines 30-31, and column 11, lines 50-52 actually discloses is:

> In communications between an SNIU user and a non-SNIU user, the above discussed Waiting Queue is employed in part to control passage of information. For example, when a SNIU receives a user datagram from a native host (non-SNIU user) which is destined for another host or user for which there is no existing association, the SNIU stores the user datagram in the Waiting Queue and transmits an association request message. When the association grant message is received, the user datagram is removed from the Waiting Queue, the corresponding Schedule table is deleted, the user datagram is encrypted and sent to the peer SNIU of the association. If an Association grant message is never received, the Schedule Table entry expires, which calls a subroutine to delete the user datagram. When a SNIU receives a user datagram from a native host, the SNIU creates an entry, if one does not already exist, in the receiving port's Association table for the source host's IP, marks the association type as `native host`, sets the security level to the receiving ports security level, and checks the opposite port's Association table for the destination's IP address. As discussed above, if an Association Table entry exists for the destination and the association type is a bona fide `native host`, the SNIU compares source and destination security levels to determine if an intended datagram can be allowed to proceed 708. If a write up situation, the SNIU along with an anticipated message releases the intended datagram. If a write down situation, the SNIU determines if the datagram was predicted and sends or audits the anticipated message as described above. If a write equal, the datagram is released to the destination.

That is, Holden at this paragraph, discloses a 'Waiting Queue' used by a serial network interface unit ('SNIU') to store user-data grams until an association is established between the SNIU and the destination user through an exchange of association request and grant messages. Holden's 'Waiting Queue,' however, does not disclose the buffer as claimed in the present application because the buffer as claimed in the present application effectively stores data until a computer's network connection is changed from a connection lacking the required security control to a connection having the required security control. Holden only discloses holding data until establishing an association with a destination user – not sending data upon a change from a network connection lacking the required security control to a connection having the required security control as claimed here. In fact, Holden is not concerned with, and therefore does not disclose, a changed computing environment having a new type of connection as claimed in the present invention. Holden therefore neither discloses nor suggests storing the data in a buffer instead of sending the data across the network if the connection to the network lacks a security control required for the determined security level of the data and sending the data from the buffer when the computer is connected to a changed computing environment having a new type of connection that has the security control required for the data as claimed here. The Office Action therefore cannot establish a prima facie case of obviousness. The rejections of under 35 U.S.C. § 103 should be withdrawn, and the claims should be allowed.

The Proposed Combination Of Herrero And Holden Does Not Teach Or Suggest Each And Every Element Of Claim 11 Of The Present Application

Independent claim 11 of the present application recites:

> 11. A method for providing a necessary level of security for a computer capable of connecting to different computing environments, the method comprising:
>
> connecting the computer to a network in a first computing environment;
>
> specifying a security level for data to be sent across the network;

> instructing a sending program to send the data across the network;
>
> receiving an indication that security control of the first computing environment lacks a security control required for the specified security level;
>
> connecting the computer to the network in a second computing environment, wherein the second computing environment has the security control required for the specified security level; and
>
> receiving an indication that the data has been sent across the network.

Herrero Neither Discloses Nor Suggests Connecting The Computer The Network In A Second Computing Environment

The Office Action takes the position that Herrero at page 4, lines 5-20, discloses the fifth element of claim 11 of the present application: connecting the computer to the network in a second computing environment, wherein the second computing environment has the security control required for the specified security level. Appellants respectfully note in response, however that what Herrero at the page 4, lines 5-20, in fact discloses is:

> According to an exemplary embodiment of the present invention, these and other objects are met by a method and apparatus for secure communication between entities in one or more networks. A determination is made whether security measures needed for the communication exist between the entities. If such measures do not exist, the security measures are established, and the communication is initiated. The security measures include security bindings including information needed for the secure communication.
>
> Security measures are established between entities in one or more networks based on predetermined security requirements and on a determined needed security level. The security level needed may be determined based on whether the entities are in the same network or in different networks and/or on the information being transmitted. Security bindings are established between the entities depending on the information to be transmitted and/or the network to which the entities belong. The security bindings include information identifying the security binding, encryption information, authentication information, integrity information, a list of addresses or group of addressees included in the security bindings, and/or information regarding the lifetime of the security bindings.

> The encryption, authentication, and integrity may be specified at a parameter level.

That is, Herrero at page 4, lines 5-20, discloses secure communication between entities in one or more networks. Herrero provides such secure communication by determining whether security measures needed for communication between entities exist, and if not, establishing such measure with security bindings. That is, Herrero only discloses secure communications through use of security bindings between entities on a network – not by connecting a computer to a second computing environment. In fact, Herrero never once discloses, mentions, or even contemplates providing a necessary level of security for a computer by connecting the computer to a second computing environment as claimed here, that is, by changing the connection between a computer and a network from a first computing environment to a second computing environment. As such, Herrero does not disclose or suggest connecting the computer to the network in a second computing environment, wherein the second computing environment has the security control required for the specified security level as claimed in the present application. The Office Action therefore cannot establish a prima facie case of obviousness. The rejections under 35 U.S.C. § 103 should be withdrawn, and the claims should be allowed.

Relations Among Claims

Independent claims 14 and 24 are system claims for providing a necessary level of security for a computer capable of connecting to different computing environments corresponding to independent claims 1 and 11 that include "means for" providing a necessary level of security for a computer capable of connecting to different computing environments. Independent claims 27 and 37 are computer program product claims for providing a necessary level of security for a computer capable of connecting to different computing environments corresponding to independent claims 1 and 11 that include "means, recorded on [a] recording medium, for" providing a necessary level of security for a computer capable of connecting to different computing environments. For the same reasons that the proposed combination of Herrero and Holden does not disclose or suggest the limitations of claims 1 and 11, the proposed combination of Herrero and

Holden also does not disclose or enable systems and computer program products corresponding to independent claims 14, 24, 27, and 37. Independent claims 14, 24, 27, and 37 are therefore patentable and should be allowed.

Dependent claims 2-10 depend from independent claim 1. Dependent claims 12 and 13 depend from independent claim 11. Dependent claims 15-23 depend from independent claim 14. Dependent claims 25 and 26 depend from independent claim 24. Dependent claims 28-36 depend from independent claim 27. Dependent claims 38 and 39 depend from independent claim 37. Each dependent claim includes all the limitations of the independent claim from which it depends. In rejecting dependent claims 2-10, 12, 13, 15-23, 25, 26, 28-36, 38, and 39, the Office Action relies on the combination of Herrero and Holden as disclosing each and every element of independent claims 1, 11, 14, 24, 27, and 37. As shown above, the combination of Herrero and Holden in fact does not disclose each and every element of independent claims 1, 11, 14, 24, 27, and 37. Because the proposed combination of Herrero and Holden does not disclose each and every element of independent claims 1, 11, 14, 24, 27, and 37, the proposed combination of Herrero and Holden cannot possibly disclose each and every element of dependent claims 2-10, 12, 13, 15-23, 25, 26, 28-36, 38, and 39. The proposed combination of Herrero and Holden, therefore, cannot establish a prima facie case of obviousness, and the rejections of dependent claims 2-10, 12, 13, 15-23, 25, 26, 28-36, 38, and 39 under U.S.C. § 103(a) should also be withdrawn.

Argument Regarding The Second Ground Of Rejection: Claims 1, 14, And 27 Are Rejected Under 35 U.S.C. § 103(A) As Being Unpatentable Over Herrero In View Of Ueda

Claims 1, 14, and 27 stand rejected for obviousness under 35 U.S.C § 103(a) as being unpatentable over Herrero in view of Ueda (U.S. Patent No. 5,692,179) (hereafter 'Ueda'). The question of whether Applicants claims are obvious or not is examined in light of: (1) the scope and content of the prior art; (2) the differences between the claimed invention and the prior art; (3) the level of ordinary skill in the art; and (4) any relevant secondary considerations, including commercial success, long felt but unsolved needs, and failure of others. *KSR Int'l Co. v. Teleflex Inc.*, 127 S.Ct. 1727, 1729-1730, 82 USPQ 1385 (2007). Although Applicants recognize that such an inquiry is an expansive and flexible one, the Office Action must nevertheless demonstrate a prima facie case of obviousness to reject Applicants claims under for obviousness under 35 U.S.C. § 103(a). *In re Khan*, 441 F.3d 977, 985-86 (Fed. Cir. 2006). To establish a prima facie case of obviousness, the proposed combination of Herrero and Ueda must teach or suggest all of Applicants' claim limitations. MPEP 2142 (citing *In re Royka*, 490 F.2d 981, 985, 180 USPQ 580, 583 (CCPA 1974)).

Ueda Neither Discloses Nor Suggests Storing The Data In A Buffer Or Sending the Data From The Buffer

The Office Action admits that Herrero does not disclose the third and fourth elements of claim 1 of the present application and to cure this deficiency of Herrero, takes the position that Ueda at column 4, lines 59-62 discloses these elements:

> storing the data in a buffer instead of sending the data across the network if the connection to the network lacks a security control required for the determined security level of the data; and
>
> sending the data from the buffer when the computer is connected to a changed computing environment having a new type of connection that has the security control required for the data.

Appellants respectfully note in response, however that what Ueda at column 4, lines 59-62, in fact discloses is:

> The judging means judges whether the security level of the inquirer and the security level of the retrieved data are in conformity with each other or not. When the security level of the inquirer and the security level of the retrieved data are in conformity with each other, retrieved results of the retrieved data are temporarily stored to the buffer means and are transmitted to a terminal on an inquirer side through the network.

That is, Ueda at column 4, lines 59-62, discloses temporarily storing data retrieved from a database at the request of an inquirer temporarily in a buffer and transmitting the retrieved data to the inquirer's terminal through a network. Ueda's temporary storage of data in a buffer and transmission of the data from the buffer does not disclose storing data in a buffer and sending the data from the buffer when a computer is connected to a changed computing environment having a new type of connection as claimed in the present application. Ueda at most discloses a well known method of data communications, used in many standard data communications protocols, in which data is stored in a buffer prior to transmission across a network. In many implementations of the common TCP/IP data communications protocol, data is stored in a buffer prior to being packetized for transmission across a network. Ueda does not disclose, however, storing data in a buffer on a computer until the computer's network connection is changed to one having a security control required for the data, evidenced by the fact that Ueda is only concerned with the security level of an inquirer, a user, a person, with respect to requested data, not the security level of a network connection. Ueda therefore neither discloses nor suggests storing the data in a buffer instead of sending the data across the network if the connection to the network lacks a security control required for the determined security level of the data and sending the data from the buffer when the computer is connected to a changed computing environment having a new type of connection that has the security control required for the data as claimed here. The Office Action therefore cannot establish a prima facie case of obviousness. The rejections of under 35 U.S.C. § 103 should be withdrawn, and the claims should be allowed

Relations Among Claims

As previously discussed, independent claims 14 and 27 are system and computer program product claims for providing a necessary level of security for a computer capable of connecting to different computing environments corresponding to independent claim 1 that include "means for" and "means, recorded on [a] recording medium, for" providing a necessary level of security for a computer capable of connecting to different computing environments. For the same reasons that the proposed combination of Herrero and Ueda does not disclose or suggest the limitations of claim 1, the proposed combination of Herrero and Ueda also does not disclose or suggest systems and computer program products corresponding to independent claims 14 and 27. Independent claims 14 and 27 are therefore patentable and should be allowed.

Conclusion of Appellants' Arguments

Claims 1-39 stand rejected for obviousness under 35 U.S.C. § 103 as being unpatentable over Herrero in view of Holden. For the reasons set forth above, however, the proposed combination of Herrero and Holden fails to establish a prima face case of obviousness. The rejection of claims 1-39 should therefore be withdrawn, and the claims should be allowed. Reconsideration of claims 1-39 in light of the present remarks is respectfully requested.

Claims 1, 14, and 27 additionally stand rejected for obviousness under 35 U.S.C. § 103 as being unpatentable over Herrero in view of Ueda. For the reasons set forth above, however, the proposed combination of Herrero and Ueda fails to establish a prima facie case of obviousness. The rejection of claims 1, 14, and 27 should therefore be withdrawn, and the claims should be allowed. Reconsideration of claims 1, 14, and 27 in light of the present remarks is respectfully requested.

The Commissioner is hereby authorized to charge or credit Deposit Account No. 50-3533 for any fees required or overpaid.

Respectfully submitted,

Date: December 5, 2008

By:

Brandon C. Kennedy
Reg. No. 61,471
Biggers & Ohanian, LLP
P.O. Box 1469
Austin, Texas 78767-1469
Tel. (512) 472-9881
Fax (512) 472-9887
ATTORNEY FOR APPELLANTS

APPENDIX OF CLAIMS
ON APPEAL IN PATENT APPLICATION OF
SUSANN M. KEOHANE, ET AL., SERIAL NO. 10/677,660

CLAIMS

What is claimed is:

1. A method for providing a necessary level of security for a computer capable of connecting to different computing environments, the method comprising:

monitoring a type of connection between the computer and a network in a current computing environment;

determining a security level of data before sending the data across the network;

storing the data in a buffer instead of sending the data across the network if the connection to the network lacks a security control required for the determined security level of the data; and

sending the data from the buffer when the computer is connected to a changed computing environment having a new type of connection that has the security control required for the data.

2. The method of claim 1 wherein monitoring a type of connection comprises periodically determining the type of connection between the computer and the network.

3. The method of claim 1 wherein monitoring a type of connection comprises event-driven determining of the type of connection between the computer and the network.

4. The method of claim 3 wherein the steps of the method are carried out by a software process and event-driven determining of the type of connection is carried out whenever the process is invoked.

5. The method of claim 3 wherein determining a security level results in a determination that data to be transmitted requires at least some level of security and event-driven determining of the type of connection is carried out in response to such determination.

6. The method of claim 1 wherein determining a security level of data before sending the data across the current network comprises reading the security level of data from a markup element embedded in the data.

7. The method of claim 1 wherein determining a security level of data before sending the data across the current network comprises reading the security level of data from meta-data in a header in a network message.

8. The method of claim 1 further comprising returning a non-fatal error to a sending program if the connection to the network lacks a security control required for the data.

9. The method of claim 8 further comprising the sending program's informing a user that the data will be held in a security buffer until the computer is connected to a changed computing environment having a new type of connection that has the security control required for the data.

10. The method of claim 8 further comprising the sending program's prompting a user with the option to create a secure tunnel for transmission of the data.

11. A method for providing a necessary level of security for a computer capable of connecting to different computing environments, the method comprising:

connecting the computer to a network in a first computing environment;

specifying a security level for data to be sent across the network;

instructing a sending program to send the data across the network;

receiving an indication that security control of the first computing environment lacks a security control required for the specified security level;

connecting the computer to the network in a second computing environment, wherein the second computing environment has the security control required for the specified security level; and

receiving an indication that the data has been sent across the network.

12. The method of claim 11 further comprising:

determining, when the computer is connected to the second network, that the second computing environment has the security control required for the specified security level; and

automatically sending the data across the network promptly upon determining that the second computing environment has the security control required for the specified security level.

13. The method of claim 11 further comprising:

receiving an indication that the second computing environment has the security control required for the specified security level; and

again instructing the sending program to send the data across the network.

14. A system for providing a necessary level of security for a computer capable of connecting to different computing environments, the system comprising:

means for monitoring a type of connection between the computer and a network in a current computing environment;

means for determining a security level of data before sending the data across the network;

means for storing the data in a buffer instead sending the data across the network if the connection to the network lacks a security control required for the determined security level of the data; and

means for sending the data from the buffer when the computer is connected to a changed computing environment having a new type of connection that has the security control required for the data.

15. The system of claim 14 wherein means for monitoring a type of connection comprises means for periodically determining the type of connection between the computer and the network.

16. The system of claim 14 wherein means for monitoring a type of connection comprises means for event-driven determining of the type of connection between the computer and the network.

17. The system of claim 16 wherein elements of the system are operated by a software process and means for event-driven determining of the type of connection is operated whenever the process is invoked.

18. The system of claim 16 wherein operation of the means for determining a security level results in a determination that data to be transmitted requires at least some level of security and means for event-driven determining of the type of connection operates in response to such determination.

19. The system of claim 14 wherein means for determining a security level of data before sending the data across the current network comprises means for reading the security level of data from a markup element embedded in the data.

20. The system of claim 14 wherein means for determining a security level of data before sending the data across the current network comprises means for reading the security level of data from meta-data in a header in a network message.

21. The system of claim 14 further comprising means for returning a non-fatal error to a sending program if the connection to the network lacks a security control required for the data.

22. The system of claim 21 further comprising means for the sending program to inform a user that the data will be held in a security buffer until the computer is connected to a changed computing environment having a new type of connection that has the security control required for the data.

23. The system of claim 21 further comprising means for the sending program to prompt a user with the option to create a secure tunnel for transmission of the data.

24. A system for providing a necessary level of security for a computer capable of connecting to different computing environments, the system comprising:

means for connecting the computer to a network in a first computing environment;

means for specifying a security level for data to be sent across the network;

means for instructing a sending program to send the data across the network;

means for receiving an indication that security control of the first computing environment lacks a security control required for the specified security level;

means for connecting the computer to the network in a second computing environment, wherein the second computing environment has the security control required for the specified security level; and

means for receiving an indication that the data has been sent across the network.

25. The system of claim 24 further comprising:

means for determining, when the computer is connected to the second network, that the second computing environment has the security control required for the specified security level; and

means for automatically sending the data across the network promptly upon determining that the second computing environment has the security control required for the specified security level.

26. The system of claim 24 further comprising:

means for receiving an indication that the second computing environment has the security control required for the specified security level; and

means for again instructing the sending program to send the data across the network.

27. A computer program product for providing a necessary level of security for a computer capable of connecting to different computing environments, the computer program product comprising:

a recording medium;

means, recorded on the recording medium, for monitoring a type of connection between the computer and a network in a current computing environment;

means, recorded on the recording medium, for determining a security level of data before sending the data across the network;

means, recorded on the recording medium, for storing the data in a buffer instead sending the data across the network if the connection to the network lacks a security control required for the determined security level of the data; and

means, recorded on the recording medium, for sending the data from the buffer when the computer is connected to a changed computing environment having a new type of connection that has the security control required for the data.

28. The computer program product of claim 27 wherein means for monitoring a type of connection comprises means, recorded on the recording medium, for periodically determining the type of connection between the computer and the network.

29. The computer program product of claim 27 wherein means for monitoring a type of connection comprises means, recorded on the recording medium, for event-driven determining of the type of connection between the computer and the network.

30. The computer program product of claim 29 wherein elements of the system are operated by a software process and the means for event-driven determining of the type of connection is executed whenever the process is invoked.

31. The computer program product of claim 29 wherein execution of the means for determining a security level results in a determination that data to be transmitted requires at least some level of security and means for event-driven determining of the type of connection executes in response to such determination.

32. The computer program product of claim 27 wherein means for determining a security level of data before sending the data across the current network comprises means, recorded on the recording medium, for reading the security level of data from a markup element embedded in the data.

33. The computer program product of claim 27 wherein means for determining a security level of data before sending the data across the current network comprises means, recorded on the recording medium, for reading the security level of data from meta-data in a header in a network message.

34. The computer program product of claim 27 further comprising means, recorded on the recording medium, for returning a non-fatal error to a sending program if the connection to the network lacks a security control required for the data.

35. The computer program product of claim 34 further comprising means, recorded on the recording medium, for the sending program to inform a user that the data will be held in a security buffer until the computer is connected to a changed

computing environment having a new type of connection that has the security control required for the data.

36. The computer program product of claim 34 further comprising means, recorded on the recording medium, for the sending program to prompt a user with the option to create a secure tunnel for transmission of the data.

37. A computer program product for providing a necessary level of security for a computer capable of connecting to different computing environments, the computer program product comprising:

a recording medium;

means, recorded on the recording medium, for connecting the computer to a network in a first computing environment;

means, recorded on the recording medium, for specifying a security level for data to be sent across the network;

means, recorded on the recording medium, for instructing a sending program to send the data across the network;

means, recorded on the recording medium, for receiving an indication that security control of the first computing environment lacks a security control required for the specified security level;

means, recorded on the recording medium, for connecting the computer to the network in a second computing environment, wherein the second computing environment has the security control required for the specified security level; and means, recorded on the recording medium, for receiving an indication that the data has been sent across the network.

38. The computer program product of claim 37 further comprising:

means, recorded on the recording medium, for determining, when the computer is connected to the second network, that the second computing environment has the security control required for the specified security level; and

means, recorded on the recording medium, for automatically sending the data across the network promptly upon determining that the second computing environment has the security control required for the specified security level.

39. The computer program product of claim 37 further comprising:

means, recorded on the recording medium, for receiving an indication that the second computing environment has the security control required for the specified security level; and

means, recorded on the recording medium, for again instructing the sending program to send the data across the network.

APPENDIX OF EVIDENCE
ON APPEAL IN PATENT APPLICATION OF
SUSANN M. KEOHANE, ET AL., SERIAL NO. 10/677,660

This is an evidence appendix in accordance with 37 CFR § 41.37(c)(1)(ix).

There is in this case no evidence submitted pursuant to 37 CFR §§ 1.130, 1.131, or 1.132, nor is there in this case any other evidence entered by the examiner and relied upon by the appellants.

RELATED PROCEEDINGS APPENDIX

This is a related proceedings appendix in accordance with 37 CFR § 41.37(c)(1)(x).

There are no decisions rendered by a court or the Board in any proceeding identified pursuant to 37 CFR § 41.37(c)(1)(ii).